SECURING AGAINST INTRUDERS AND OTHER THREATS
THROUGH A NFV-ENABLED ENVIRONMENT

[H2020 - Grant Agreement No. 700199]

Deliverable D6.2

Standardization Plan

Editor Antonio Pastor (TID)

Contributors Jeronimo Nuñez, Diego R. Lopez (TID), Ludovic Jacquin (HPELB), Dimitris Katsianis (INCITES), Eleni Trouva (NCSRD), Carolina Fernandez (I2CAT), Olga Segou (ORION), Antonio Lioy (POLITO)

Version 1.0

Date April 30th, 2017

Distribution PUBLIC (PU)

Executive Summary

This document provides the initial plans of the SHIELD project for standardization activities, as one of the ways to achieve the industrial impact that the project should have, fulfilling its main objectives.

The plan is organized in two areas; first, the bodies and industrial associations with standardization capacity or influence, and, second, the open-source initiatives with the capacity of being adopted by previous organizations or being considered as standards (de facto).

In the first area, SHIELD plans to focus its efforts in well-known organizations such as IETF, ETSI or IEEE, in the areas related to Network Virtualization and Security, which are both key assets of SHIELD project. Furthermore, additional associations (TM Forum and MEF) are in the radar.

For the second area, the plan includes the participation in several existing open-source projects in two different ways: promoting the results of SHIELD (attestation, framework, APIs, etc.) to be adopted, or directly adopting, modifying and contributing to the code. In both cases, we can mention OSM and T-NOVA TeNOR as the most relevants to NFV orchestrators, Apache Spot could be considered as a novel framework for security data analysis, and Docker is considered to be the reference in containers management application.

Finally, the deliverable includes the KPIs and the planning to accomplish the standardization objectives, including the different ways of sizing the KPIs.

Table of Contents

1. INTRODUCTION

This document has a twofold objective: first, to identify the list of potential standardization organizations and open-source initiatives; and, second, to elaborate and seize a realistic planning to achieve a significant impact in the most relevant of them. This list has been created with the cooperation of the partners and includes those of them who can benefit from the SHIELD results. This is the initial exercise in SHIELD related with T6.2, “Contribution to standard bodies and international fora", as part of WP6.

The structure of the document is as follows:

- Section 2 includes a detailed list of potential standardization organizations, a brief description of them, and underlines where and how SHIELD can contribute.
- Section 3 performs a similar exercise but focused on open-source initiatives, as “de facto” standards and/or reference implementations of formal ones.
- Section 4, presents the planning and KPIs to be accomplished during project lifetime.
- Appendix A. includes a reference of achievements already obtained in the project.

2. STANDARDIZATION ORGANIZATIONS

This section enlists and elaborates the set of standardization organizations identified in this analysis and strategy phase by consortium members. The different organizations have been structured around some main categories. For each standardization organization, a set of potential groups or activities are proposed as suitable for standardisation activities for SHIELD project.

2.1. Internet and ICT-related

2.1.1. IETF/IRTF

The Internet Engineering Task Force (IETF) is a large open international organization, which is the meeting place for Internet network designers and providers, vendors, and researchers focusing on the evolution of the Internet architecture and its operation. It is open to any interested individual. The IETF Mission Statement and tao ("path") guide is documented in RFC 3935 and RFC4677 respectively. The IRTF (Internet Research Task Force) is a parallel organization focusing on longer term research issues, and RFC 4440 provides further details on its role.

The standardization process is based on the following elements:

- IETF meetings - which are held three times per year, as well as via mailing lists. Much of the work is done through these IETF meetings. IETF contributions and decisions are considered made and decided by individuals. Any individual can attend an IETF meeting. Both registration and payment of a registration fee are essential in order to attend an IETF meeting.
- Working Groups - Working Groups are formed around a charter describing their objectives and plans. They have at least two co-chairs responsible to promote the completion of the WG charter, moderate discussions, and evaluate and declare WG consensus. WGs are clustered in seven functional areas, with at least two Area Directors per area. The current IETF areas are Applications and Real-time, Internet, Operations and Management, Routing, Security, Transport, and a General area focused on the coordination with IANA. The IRTF has a similar structure, but the equivalent to WGs are called Research Groups (RG) and there are no areas.
- BOFs – There are face-to-face meetings inside an IETF meeting to discuss the opportunity of starting a new WG, whenever there are some individuals who are interested on the same topic in a particular area that is not covered by an existing WG. Such meetings are called Birds of a Feather meetings (BOFs) and have to be approved by the Area Director in the relevant area before it can be scheduled. Moreover, a mailing list could also be set up, where all participants could start discussing and working on the topic.
- RFCs and Internet Drafts – Every IETF standard is published as a Request for Comments (RFC) and every RFC starts out as an Internet Draft (I-D). The procedure in order to publish a standard is the following:

- Publish the document as an Internet Draft.
- Receive comments on the draft and edit the draft based on the comments.
- Repeat the steps above, until the draft is efficiently discussed. Then it is submitted to the IESG.

If the IESG approves, the draft is published as a proposed standard and after six months it can become a draft standard. A few years after a document has been a draft standard, it can become an Internet standard. The IRTF follows a similar process, that becomes an experimental RFC and the body in charge of approving it is termed IRSG.

The list of Working Groups where SHIELD consortium foresees opportunities to channel results can be found below:

- I2NSF WG: The goal of I2NSF is to define a set of software interfaces and data models for controlling and monitoring aspects of physical and virtual NSFs, enabling clients to specify rulesets. This group is a clear target for potential results in platform and function attestation, and security policy specifications and data models.
- OPSA WG: The Operations and Management Area development and publication of RFCs dealing with operational and management topics. SHIELD can contribute in the area of operational interface for security management.
- NFV RG: The NFVRG focuses on research problems associated with NFV-related topics. It brings together researchers from both academia and industry to explore the research problems related to NFV. Reports on project results, especially in composition of security network services and data-driven management will be proposed by the consortium.
- ACME WG. The Automated Certificate Management Environment (ACME) working group is specifying ways to automate certificate issuance, validation, revocation and renewal. ACME applicability for temporal certificate issuance to allow vNSFs to monitor and report security incidents over encrypted traffic is targeted by the consortium and results will be promoted in the WG.

2.1.2. OASIS

OASIS is a non-profit organisation that steers the development of open standards for the global information society. OASIS promotes industry convergence as well as the adoption of worldwide standards for a multitude of areas such as security, privacy, Internet of Things, cloud computing, energy, content technologies, emergency management, etc. OASIS open standards offer the potential to “lower cost, stimulate innovation, grow global markets, and protect the right of free choice of technology”. OASIS currently has more than 5,000 participants across 600 industries, organizations and individual members. Some OASIS-developed standards with relevance to SHIELD, include:

- TOSCA-v1.0 [1]. Topology and Orchestration Specification for Cloud Applications.
- TOSCA-Simple-Profile-YAML-v1.0 [2]. TOSCA Simple Profile in YAML.
- CAMP-v1.1 [3]. Cloud Application Management for Platforms Version 1.1.
- CAMP-Test-Assertions-v1.1 [4]. Cloud Application Management for Platforms (CAMP) Test Assertions Version 1.1.

- xacml-dlp-nac-v1.0 [5]. XACML Data Loss Prevention / Network Access Control (DLP/NAC) Profile Version 1.0.

Therefore, possible contributions to OASIS are: recommendations for Trusted Computing, Attestation and the orchestration templates used by the SHIELD VNF Orchestrator.

2.2. Network and Management-related

2.2.1. ETSI NFV ISG

ETSI is the European Telecommunication Institute, a Standards Organization recognized by the European Union, and focused on producing global standards for Information and Communications Technologies (ICT), including fixed, mobile, radio, converged, broadcast and Internet technologies. ETSI has more than 800 member organizations in 64 countries all over the world, and among the most salient standards produced by ETSI we can cite the ones around GSM, DECT, or smart cards.

ETSI has evolved a well proven standards-making process, which ensures published standards are of high quality and are produced in an efficient manner. Specifically:

- Most of the standardization work is carried out by committees. The members of these committees are technical experts from member organizations. These committees meet typically between two and six times a year, either at ETSI premises or elsewhere. There is a range of different types of committees for different tasks:
    - Technical Committees (TC) and ETSI Projects (EP). Both activities are defined in their terms of reference. TCs work in a specific technology area, while EPs are established in a fixed period of time to meet particular market sector needs.
    - ETSI Partnership Projects, established when there is a need to co-operate with other organizations to achieve a standardization goal. There are currently two Partnership Projects: The Third Generation Partnership Project (3GPP) and oneM2M.
    - Industry Specification Groups (ISG), operating alongside the traditional standards- making mechanisms and focusing on a very specific activity. ISGs are self-contained, decide their own work programme and approve their own specifications.
- The ETSI Directives define the legal status, purpose, scope, and functions of ETSI and covers the entire lifecycle of their standards.
- ETSI committees are coordinated by the Operational Co-ordination Group (OCG), which includes the chairmen of all our technical committees. Ultimately the committees are accountable to the ETSI Board and the General Assembly.
- ETSI members decide what work to be done, by each committee establishing and maintaining a work programme which is made up of individual items of work. Collectively, the work programmes of all the committees constitute the ETSI Work Programme. Each work item describes a specific standardization task and normally results in a single standard, report or another document.

- ETSI follows an open approach to standardization, and operates by direct participation (ETSI members are not represented by a national delegation or other body), and any member may bring as many contributions and voice as many opinions as desired. Decisions are taken by consensus, declared by the committee plenary.

ETSI promotes the introduction of standardization as early as possible in the development of a new technology, as it would provide a solid foundation for its future exploitation.

SHIELD intends to begin early standardization and pre-standardization activities in ETSI, specifically in the committee of highest relevance to the project, the ISG on Network Functions Virtualization. The following list describes the different working groups in which the ETSI NFV ISG is organized and describes the main contributions SHIELD can make to each one of them.

- WG SEC is the security group that addresses aspects related to information, network and communications security, individual machines/processes, tools, controls and techniques. It addresses security at design-time, deployment-time and run-time, and the appropriate measures for operational efficiency and features to support regulatory requirements, e.g. Lawful Intercept, Privacy and Data Protection. SHIELD plans to promote its results in the work-items related to security monitoring and orchestration. Also, the results in Remote Attestation (RA), used in SHIELD to monitor the software integrity of the nodes hosting the vNSFs, will be presented for possible standardization in this group.
- WG EVE, the Evolution and Ecosystem WG, includes several areas of activity, such as the identification of new use cases, or evaluating new technologies. SHIELD plans to contribute to use cases and reports focused on data-driven management.
- WG TST is focused on testing and implementation issues, especially focused on interoperability. Plans include the participation in relevant PoCs demonstrating SHIELD results.
- WG IFA (Interfaces and Architecture) activity is oriented to normative aspects, such as architectures, interoperability at reference points and information models. A potential interface extension required to support the DARE is considered an interesting opportunity for contribution.
- WG SOL (Solutions) is committed to deliver a set of protocols and data models specifications. SHIELD could provide potential data model extensions required to provide the DARE functionalities.

In summary, it is expected to contribute in aspects and features related to security orchestration and data-driven management.

2.2.2. TM Forum

TM Forum is a global industry association for digital business transformation. TM Forum encompasses more than 900 market-leading organizations. Its main goal is to provide frameworks, tools, reports, use cases and demonstrations, to ease the digital transformation and ensure consensus around it. The three TMF pillars are the following:

- Agile and Virtualized: to capture the transformation of the IT and operations that are accelerating research and development, ensuring the improvement of the business agility for the industry of ICT while reducing costs and risks.

- Open and Partner effectively: to capture the smooth delivery, integration and management with partners.
- Customer Centric: to capture the engagement of improving the experience of customers.

TM Forum fosters developing best practices and standards through joint work or exchange of live collaboration materials with other TM Forum projects. To make collaboration between such projects easier, TM Forum has grouped several projects together in a Core Project Area. Some of the relevant projects with common ground with SHIELD are:

- Data Analytics. This project aims to introduce the use of Big Data and Big Data Analytics within the business of the service provider.
- Zoom (Zero-touch Orchestration, Operations and Management) Project. This project targets to define agile and flexible management operations to enable the delivery and management of physical and virtual resources and services while ensuring lower capital and operational expenditures.

SHIELD will also explore potential Catalyst projects. Catalysts are proof-of-concept projects developed collaboratively by TM Forum members. These projects bring together large and small companies in order to create innovate solutions to common challenges.

2.2.3. IEEE

The Institute of Electrical and Electronics Engineers (IEEE) is the biggest professional association around the world with more than 400,000 members distributed in different chapters. Between their activities includes Standardization, through IEEE-SA (IEEE Standards Association) which is focused on the development of internationally recognized standards.

SHIELD activities will be focused in monitoring the evolution of the proposals made to IEEE related to encrypted traffic management and the potential of new protocols, such as Multi-Context TLS (mcTLS), proposed in section 3.2.2.

2.2.4. MEF

The MEF, founded in 2001 as the Metro Ethernet Forum, is a non-profit international industry consortium. Today MEF facilitates industry-neutral implementation environments for service orchestration (OpenLSO) and L2-L7 connectivity services (OpenCS) based on open-source reference implementations, SDN and NFV, as well as current commercial PNF products. MEF operates as a mix between technical and marketing forum, making recommendations to existing standards bodies. It provides certification programs and educational resources.

MEF promotes developing and implementing agile, assured and orchestrated “Third Network services” for the digital economy and the hyper-connected world. Orchestrated Cloud Service is one of them and in this area SECaaS (Security as a Service) is the first project in progress. Experiences with the SHIELD user and (possibly) inter-domain interfaces, will be reported to MEF's SECaaS initiative through liaison or open-source sharing.

2.3. Security-related

2.3.1. ETSI CYBER

Cyber Security (CYBER) is one of the above mentioned (section 2.2.1) ETSI Technical Committees (TC), created as the ETSI centre of expertise in the area of cybersecurity to assist all ETSI Groups with the development of cybersecurity requirements. CYBER responsibilities include developing and maintaining the standards, specifications and other deliverables, supporting the development and implementation of cybersecurity standardization within ETSI, collecting and specifing cybersecurity requirements from relevant stakeholders, identifing gaps where existing standards do not fulfil the requirements and providing specifications and standards to fill these gaps, without duplication of work in other ETSI committees and partnership projects, ensuring that appropriate standards are developed within ETSI in order to meet these requirements, coordinating work in ETSI with external groups such as ENISA, and answering to policy requests related to cybersecurity, and security in broad sense in the ICT sector.

SHIELD consortium will be monitoring the ETSI CYBER activities and seek opportunities for collaboration or contribution related to:

- The applicability of NFV to provide security for critical infrastructures.
- Middlebox Security Protocol (MSP) and mcTLS proposals.

2.3.2. Trusted Computing Group

The Trusted Computing Group (TCG) is a not-for-profit organization formed to develop, define and promote open, vendor-neutral, global industry standards, supportive of a hardware-based root of trust, for interoperable trusted computing platforms. Its flagship standard is the Trusted Platform Module (TPM), which is virtually included in all enterprise PCs, many servers and embedded systems. Moreover, networking equipment, drives and other devices and systems deploy other TCG specifications, including self-encrypting drives and network security specifications.

TCG is structured around a Board of Directors, Committees (such as the Technical Committee) and Work Groups (WG), with supermajority voting. The different WGs are responsible for proposing new – or errata – standards that are validated by the Technical Committee.

In addition to presenting SHIELD as a use case for the different TCG standards, the consortium foresees possible contributions to two WGs:

1. TPM WG: Definition of the implementation of the TPM architecture. TPMs are a basic building block used in most other specifications, for providing an anchor of trust. They can be used for validating basic boot properties before allowing network access, or for storing platform measurements, or for providing self-measurement to provide anchors of trust to hypervisors.
2. Network Equipment subgroup (part of the Embedded System WG): One of SHIELD's goal is to couple server and vNSF attestation with network configuration attestation. Thus, the Network Equipment subgroup is a prime contribution candidate for the consortium.

3. OPEN-SOURCE SOFTWARE INITIATIVES

In this section, a list of different open-source projects with enough maturity in the code and stakeholders presence to be bonded with SHIELD is presented.

Open-source communities have become the source for de-facto standard solutions in several areas, such as the field of NFV, security or network management. Adoption of open source solutions and collaboration with their support communities provide a number of benefits related to software development, which are especially valuable for projects with a clear focus in security that demand trust, such as SHIELD. These benefits include:

- *Security*: With thousands of developers working with full visibility on software code, it is more likely that code flaws are discovered and patched very quickly.
- *Quality*: Open source projects are supported by large communities, including experts from industry and academia, increasing the quality of the project.
- *Flexibility:* The capability to personalize the source-code adding needed features.
- *Freedom*. Open-source projects break the vendor lock-in rule.
- *Auditability:* The visibility of the code ensures that the project fully adheres to its requirements and functionality, avoiding "extra code", like backdoors or similar pieces of software.
- *Support Options:* Paid support becomes an option, not a mandatory cost.

3.1. NFV related

3.1.1. Open Source MANO (OSM)

ETSI OSM [6] is an operator-led ETSI community that is delivering a production-quality pen-source Management and Orchestration (MANO) stack, which is aligned with ETSI NFV Information Models and meets the requirements of production NFV networks.

OSM is engineered, tested and documented to allow rapid installation in operator labs worldwide that seek to create a scalable and interoperable open-source MANO environment. It substantially enhances interoperability with other components (VNFs, VIMs, SDN controllers) and creates a plug-in framework to make platform maintenance and extensions significantly easier to provide and support. The contribution of the output of its modelling work to the ETSI NFV ISG is among the goals of the OSM project.

The OSM community has defined an expansive scope for the project covering both design-time and run-time aspects related to service delivery for telecommunications service provider environments. The immediate objective is that the OSM code base can be leveraged in these environments as-is in a Roll-Your-Own context, or in whole or part of a commercial product offering.

Figure 1 shows the mapping of scope between the OSM components and the ETSI NFV MANO logical view, according to the ETSI NFV Reference Architecture Framework.

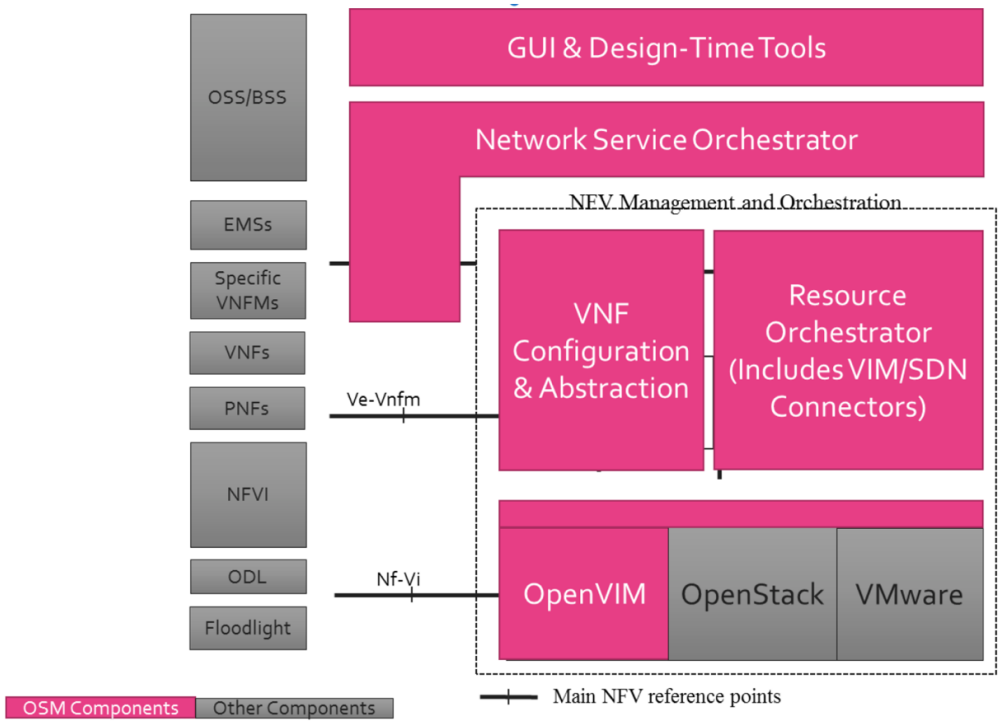

Figure 1: OSM components in the ETSI NFV Architecture Framework

The run-time scope of OSM includes:

- Automating end-to-end Service Orchestration environment that enables and simplifies the operational considerations of the various lifecycle phases involved in running a complex service based on NFV.
- Super-setting of ETSI NFV MANO where the salient additional area of scope includes Service Orchestration but also explicitly includes provision for SDN control.
- Delivering on a plug-in model for integrating multiple VIMs
- One reference VIM that has been optimized for Enhanced Platform Awareness (EPA) to enable high performance VNF deployments.
- Integrating a “Generic” VNFM with support for integrating “Specific” VNFMs.
- Facilitating support for OSM to integrate Physical Network Functions into an automated Network Service deployment.
- Being suitable for both Greenfield and Brownfield deployment scenarios.
- GUI, CLI and REST interfaces to enable access to all features.

The design-time scope of OSM includes:

- Delivering a capability for Create/Read/Update/Delete (CRUD) operations on the Network Service Definition.
- Supporting a Model-Driven environment with Data Models aligned with ETSI NFV MANO.
- Simplifying VNF Package Generation.
- Supplying a Graphical User Interface (GUI) to accelerate the network service design time phase.

OpenMANO [7] is a former open-source project that provided one of the code seeds for OSM, and currently incorporated as part of OSM Resource Orchestrator and providing the reference

VIM optimized for EPA support that is an essential part of the OSM run-time scope. OpenMANO is mainly sponsored by Telefonica, and its current software distribution consists of three main software components (Figure 2):

- openvim: Reference implementation of an NFV VIM (Virtualised Infrastructure Manager). It interfaces with the compute nodes in the NFV Infrastructure and an OpenFlow controller in order to provide computing and networking capabilities and to deploy virtual machines. It offers a northbound interface, based on REST (openvim API), where enhanced cloud services are offered including the creation, deletion and management of images, flavours, instances and networks. The implementation follows the recommendations of ETSI NFV ISG Best Practices on Performance.
- openmano: Reference implementation of an NFV-O (Network Functions Virtualisation Orchestrator). It interfaces with an NFV VIM through its API and offers a northbound interface, based on REST (OpenMANO API), where NFV services are offered including the creation and deletion of VNF templates, VNF instances, network service templates and network service instances.
- openmano-gui: Web GUI to interact with OpenMANO server, through its northbound API, in a friendly way.

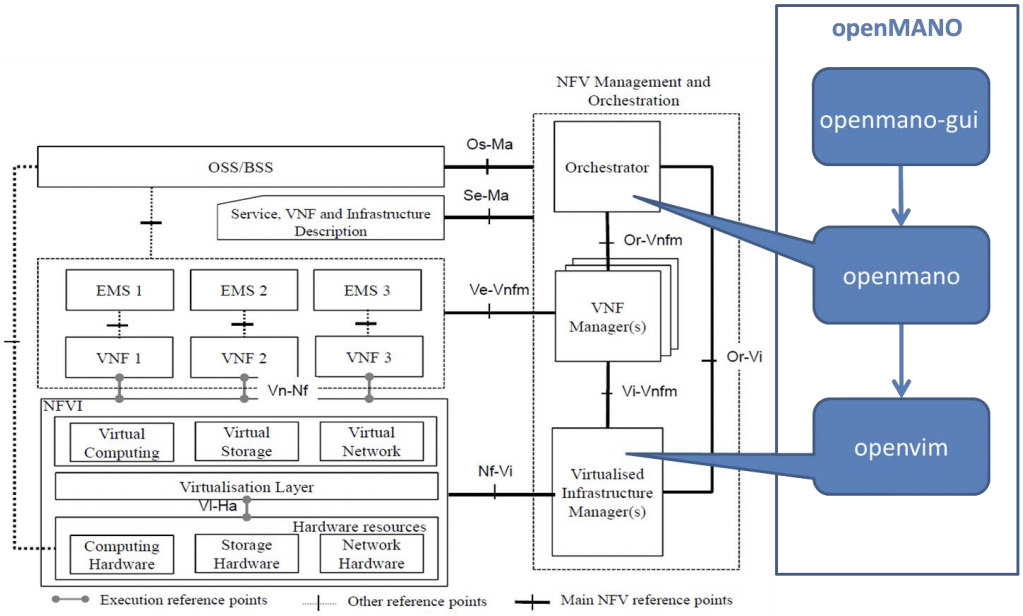

Figure 2: OpenMANO high-level architecture

The SHIELD plans for this open-source initiative will be to present to the OSM community the attestation capacity of the Trust monitor and the vNSF Orchestrator. The ideal outcome out of this standardisation activity will be the adoption of the presented SHIELD procedures and modules by the OSM community.

3.1.2. T-NOVA TeNOR Orchestrator

FP7 T-NOVA project [8] specifically focuses on the aspects of Network Functions Virtualisation (NFV), which aimed to introduce a novel enabling framework. This allowed operators not only to deploy Virtualized Network Functions (VNFs) for their own needs, but also to offer them to their customers, as value-added services. Virtual network appliances (gateways, proxies,

firewalls, transcoders, analysers, etc.) can be provided on- demand as-a-Service; eliminating the need to acquire, install and maintain specialized hardware at customers' premises.

For these purposes, T-NOVA designs and implements TeNOR, a management/orchestration platform for the automated provision, configuration, monitoring and optimization of Network Functions-as-a-Service (NFaaS) over virtualised Network/IT infrastructures. In other words, T-NOVA combines IT/cloud virtualisation and Network-as-a-Service concepts to offer a complete end-to-end Cloud Network service. The following figure presents TeNOR's high level architecture. The functional blocks represented as yellow, blue, and red are TeNOR specific functions; while the green blocks represent T-NOVA north and southbound system components.

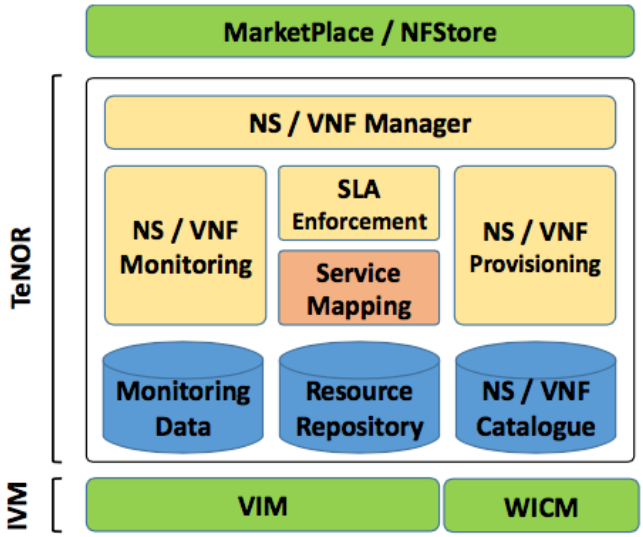

Figure 3: TeNOR high-level architecture

For TeNOR, a micro-service based architecture was selected. This ensures a lean and modular implementation and operation of the system. Micro-services are organized in two groups: one dedicated to NSs, which provides services to the upper layers (i.e. green blocks) and requests services from the second group, which is dedicated to VNF-related operations. The micro-services required for the function of TeNOR are:

1. NS/VNF Manager: it is a facade for the northbound interface (the Marketplace for the NS Manager, the NS Manager for the VNF Manager (VNFM)), which and manages the NS/VNF Catalogue. The proposed architecture embraces both the concept of generic VNFM as well as VNF specific VNFMs, as suggested by ETSI WG;
2. Service Mapping: contains the mapping algorithm implementations, which map the required resources to support a NS instance to the best available location in the infrastructure;
3. NS/VNF Provisioning: it accepts requests for NS instances from the Marketplace (through the NS Manager) and for VNF instances from the VNFM; it also manages the NS/VNF Instances repositories;
4. NS/VNF Monitoring: it accepts Virtual Machine (VM) based monitoring data from the lower virtualize infrastructure and management (VIM) layer and maps it to the corresponding NS/VNF instances. This data is later given to the Marketplace, for both Customers and Function Provider dashboards;

5. SLA Enforcement: responsible for comparing monitoring data to the agreed SLA for every NS instance, and generates alerts for impending SLA breaches. Data associated with a potential breach is passed to the NS Manager, which initiates the necessary actions to guarantee the SLA (it either migrates or scales VNF instances or improves their network connections).

Further information on TeNOR architecture and implementation can be found in [9] and in [10]. SHIELD targets the development of new features in the vNSF Orchestrator that will be shared with the TeNOR upstream. The expected modifications relate to the introduction of management schemas for the modification of the configuration in the remediation vNSFs and for sharing information on vNSFs and infrastructure details with the analytics engine, as well as the interworking with the Trust monitor for attestation purposes. These new features are expected to be useful for the communities developing and using TeNOR orchestrator.

3.1.3. Docker

Remote Attestation (RA) is the main technique used in SHIELD to monitor the software integrity (and hence the trust) of the nodes hosting the vNSFs. RA is based on the Trusted Computing paradigm, which is well-known to work well on physical platforms but has problems with virtualization environments. Currently, lightweight virtualization is one of the hot techniques for NFV environments, with special emphasis on Docker containers. Docker [11] is the world's leading software container platform. Docker allow to run and manage apps side-by-side in isolated containers to get better compute density.

SHIELD will adapt standard RA techniques to the Docker environment. Moreover, the patch required for Docker to work smoothly with RA will be published open-source and, to avoid creating a new patch for every new release of Docker, we will submit the patch to Docker maintainers seeking their approval to become officially part of the Docker codebase.

3.2. Security-related

3.2.1. Apache Spot

Apache Spot [12], formerly known as Open Network Insight (ONI), is a platform for network telemetry and anomaly detection, built on an open data model and Apache Hadoop. It is an open-source project based on the Cloudera platform; originally developed by Intel, Cloudera and other major cybersecurity analytics organizations. It was donated to the Apache Software Foundation (ASF) in 2016, thus providing a higher level of cybersecurity response, by allowing the Apache community to contribute in discovering new analytics functionalities for the detection of advanced cyber threats. Spot combines big data processing, scalable machine learning and is premised on a community-driven open data model that addresses the need for agility and decoupling of analytics from threat detection to counter constantly evolving use cases. It features threat detection, investigation and remediation capabilities via machine learning and consolidates all enterprise security data into a comprehensive IT telemetry hub.

The open-source nature of the Spot project allows for collaboration from academia, the public sector and the private sector, either by enriching commercial software or by extending its

capabilities. Furthermore, the Apache Spot community is tightly connected with the Apache Hadoop community for data collection and storage and with the Apache Spark community for ML-based anomaly detection, ensuring the high-quality result of the contributors' efforts.

SHIELD acknowledges the impact of the Spot platform in the field of cybersecurity analytics and plans to implement it as part of the DARE. In order to meet the project's requirements for a cognitive data analytics engine, the project plans to extend Spot's capabilities, while contributing to the ASF in the following manner: The anomaly detection procedure is planned to be enriched with additional machine learning algorithms that will function in parallel with the existing one, enhancing the engine's efficiency. Moreover, plans include the development of a classification algorithm that will identify the detected anomalies as specific cybersecurity threats, thus enabling the trigger of automatic task-specific remediation activities. Finally, all the useful knowledge and results from Spot's implementation that do not pertain to the Articles 27, 36, 37 and 39 of the SHIELD Grant Agreement will be communicated to the open-source communities via their collaboration tools (mailing lists, Slack channels, developer forums). Sharing the above contributions with the Spot community will not only allow for the overall improvement of the platform but may lead other organizations to adapt a more cooperative and sharing approach in terms of visibility of security data and detection methods.

3.2.2. Multi Context TLS

Multi Context TLS (mcTLS) [13] is a secure communication protocol that extends TLS to allow endpoints to incorporate trusted middleboxes into secure sessions, according to the following basic principles:

- *No Transparent Middleboxes*: Both endpoints explicitly approve each middlebox.
- *Least Privilege*: Middleboxes see only what they need to do their jobs.
- *Middlebox Authentication*: Client and server can verify the identity of each middlebox.
- *No Custom Root Certificates*: Overall security is not undermined by requiring users to install root certificates

An initial open-source version is available in [14]. Initial plans in SHIELD include to develop a proxy vNSF mcTLS/TLS in order to offer it as a security application to inspect HTTP traffic by TLS client servers. This application could be contributed to the mcTLS upstream, with the aim to demonstrate the mcTLS applicability, recently being considered by the IEEE and the ESTI CYBER TC.

4. PLANNING AND KPIS

This section defines the standardization KPIs. The aim of the SHIELD consortium is to fix as a starting point the minimum committed achievements (two different contributions in standardization groups). Nevertheless, the commitment of the partners is to expand the standardization achievements, monitoring and contributing in as many as possible organizations mentioned in the above sections, especially as a tool that allows project results to achieve a higher impact on the industry and increase exploitation opportunities.

The standardization plan to reach the KPI set in SHIELD has been defined in two stages, as it is shown in Table 1. Standardization KPI. The first stage that covers the first-year project lifetime (M1-M12) will allow partners to raise awareness of the project in different initiatives and associations, and the second Stage includes the remaining time frame (M13-M30) where SHIELD expects to transfer obtained results into the standardization and especially in open-source initiatives.

Table 1. Standardization KPIs

KPI	Stage 1 (M1-M12)	Stage 2 (M13-M30)	Total
Standardization Organizations	1	1	2
Open source initiatives	No planned	2	2

The KPI of contributions can be measured by any of the following goals:

- Contributions in SDO documents that reflect SHIELD concepts, frameworks, or results. For instance, an adopted Internet-draft in the IETF or an accepted contribution as part of a GS or GR in ETSI.
- Presentation of documents, concepts, demonstrators or results in regular meetings of standardization organizations.
- Liaisons with standardization organizations or open-source initiatives to use, adopt and receive feedback on SHIELD results.
- Source code developed within SHIELD to be integrated in upstream open-source initiatives.

Appendix A depicts first results obtained so far (April 2017) as part of the Stage 1.

5. CONCLUSIONS

The discussion on the landscape of standardisation and industry fora in the area of NFV-based cybersecurity - as well as the discussion of standardisation activities relevant to SHIELD in this standardisation plan lead to a list of interesting opportunities for the consortium, in order to provide substantial contributions to international and global standards. For each of the areas of standardisation (standard bodies, industrial associations and open-source initiatives) promising fields for contributions have been identified with an impact to international fora.

REFERENCES

[1] "OASIS Standard version 1.0". 25 November 2013, [Online], http://docs.oasis-open.org/tosca/TOSCA/v1.0/os/TOSCA-v1.0-os.html.

[2] "OASIS Standard. Version 1.0". Edited by Derek Palma, Matt Rutkowski, and Thomas Spatzier. 21 December 2016, [Online] latest version: http://docs.oasis-open.org/tosca/TOSCA-Simple-Profile-YAML/v1.0/TOSCA-Simple-Profile-YAML-v1.0.html.

[3] "CAMP version 1.1". Edited by Jacques Durand, Adrian Otto, Gilbert Pilz, and Tom Rutt. 09 November 2014. OASIS Committee Specification 01, [Online], latest version: http://docs.oasis-open.org/camp/camp-spec/v1.1/camp-spec-v1.1.html.

[4] "CAMP-Test-Assertions-v1.1". Edited by Jacques Durand, Gilbert Pilz, Adrian Otto, and Tom Rutt. 09 November 2014. OASIS Committee Specification 01, [Online], latest version: http://docs.oasis-open.org/camp/camp-ta/v1.1/camp-ta-v1.1.html.

[5] "xacml-dlp-nac-v1.0". Edited by John Tolbert, Richard Hill, Crystal Hayes, David Brossard, Hal Lockhart, and Steven Legg. 16 February 2015. OASIS Committee Specification 01, [Online], latest version: http://docs.oasis-open.org/xacml/xacml-3.0-dlp-nac/v1.0/xacml-3.0-dlp-nac-v1.0.html.

[6] "Open Source MANO" [online]. https://osm.etsi.org/, Retrieved 4/2017

[7] "OpenMANO Project" [Online], http://www.tid.es/long-term-innovation/network-innovation/telefonica-nfv-reference-lab/openmano, Retrieved 4/2017

[8] "T-NOVA FP7 project". [Online]. http://www.t-nova.eu/, Retrieved 4/2017.

[9] J. F. Riera, J. Batall, F. Liberati, A. Giuseppi, A. Pietrabissa, A. Ceselli, A. Petrini, M. Trubian, P. Papadimitrou, D. Dietrich, A. Ramos, and J. Meli, "TeNOR : Steps Towards an Orchestration Platform for Multi-PoP NFV Deployment," in Proc. of the 2016 2nd IEEE Conference on Network Softwarization (NetSoft), 2016

[10] T-NOVA project - Deliverable 3.41: Service Provisioning, Management and Monitoring – Interim, December 2015

[11] Dockers. [online], http://docker.com

[12] "Apache Spot (Incubating), A Community Approach to Fighting Cyber Threats" [Online], https://spot.incubator.apache.org, Retrieved 4/2017

[13] Naylor, D., Schomp, K., Varvello, M., Leontiadis, I., Blackburn, J., López, D. R., ... & Steenkiste, P. (2015, August). "Multi-context tls (mctls): Enabling secure in-network functionality in tls". In ACM SIGCOMM Computer Communication Review (Vol. 45, No. 4, pp. 199-212)

[14] "Multi-contex TLS github project page" [online], https://github.com/scoky/mctls, Retrieved 4/2017

LIST OF ACRONYMS

Acronym	Meaning
ETSI	European Telecommunications Standards Institute
IANA	Internet Assigned Numbers Authority
IEEE	The Institute of Electrical and Electronics Engineers
IESG	Internet Engineering Steering Group
IETF	Internet Engineering Task Force
IRTF	Internet Research Task Force
OSM	Open Source MANO
TCG	Trusted Computing Group
TLS	Transport Layer Security
TPM	Trusted Platform Module

APPENDIX A. CURRENT RESULTS

This appendix details the current results obtained from the beginning of the project to the moment of the publication of the present document.

ETSI NFV EVE Working Group contribution

SHIELD partners that are also ETSI members have submitted a document presenting the SHIELD use case (“Security as a Service Use Case”) to the ETSI NFV EVE working group. The document was approved and it will be incorporated into the new version of the ETSI NFV 001 document ("Network Functions Virtualisation (NFV); Use Cases”) as Use Case #15: Security as a Service (SecaaS).

MEF

Initial conversations are being carried out with MEF in what relates to MEF proposal of a Security-as-a-Service (SECaaS) API. The timeframe seems rather favourable to achieve a high impact, since MEF has just started the internal discussions to shape the API .